2018

A Blueprint for Online Dispute Resolution System Design

Amy J. Schmitz

University of Missouri School of Law, SCHMITZAJ@MISSOURI.EDU

A Blueprint for Online Dispute Resolution System Design

By Amy J. Schmitz

A great deal of discussion focuses on how arbitration and similar private dispute resolution harms consumers, and how businesses seek ways to avoid helping consumers.[1] It is often assumed that companies and consumers are on opposing "teams." In reality, however, consumers and companies enjoy more commonalities than contradictions. Both benefit when deals go well and disputes are resolved quickly and cheaply.

The problem is that face-to-face dispute resolution can be costly in terms of time and money. Furthermore, getting lawyers involved may inspire gamesmanship and adversarial antics aimed to protect one's reputation for staying "strong" and refusing to settle or admit wrongdoing. The solution is a well-designed online dispute resolution (ODR) system that harnesses business and consumer commonalities, and creates a win-win for all stakeholders in eCommerce disputes.[2]

That is not to say that ODR is the "end-all-be-all" for eCommerce disputes. All ODR is not fair and efficient. In fact, it is tempting to slip into cynicism about ODR and the fate of consumers on the Internet. Consumers assume that businesses will always have the power —as if bad consumer experiences are inevitable. Some also assume that merchants who provide internal ODR systems for solving eCommerce claims must have a hidden agenda, or unfair disadvantage.

Such assumed negativity regarding ODR is wrong. The Internet undoubtedly generates vulnerabilities for consumers, but it also creates opportunities for consumer empowerment. The time is right to take advantage of those opportunities. Merchants, payments providers, consumer groups, regulators, and other policymakers must join forces in addressing this challenge by creating a unified ODR system that provides fast and fair resolutions worldwide. Aiming to catalyze this effort, this essay will address design caveats and provide criteria for creating a just ODR system.

ADDRESSING ASYMMETRIES

There are many considerations for designing a just ODR system. The first is to address asymmetries that tilt the playing field in favor of merchants. Often commentators and policymakers discuss these asymmetries in terms of "repeat player advantages," which have been documented and debated for quite some time with respect to arbitration, for example. This focuses on the fact that merchants generally are repeat players in dispute resolution processes, and thus gather information that gives them an advantage in resolving disputes toward their favor. Furthermore, these repeat player merchants usually have greater legal and financial resources than consumers, again causing the system to tilt in the merchants' favor.

Said another way, merchants and consumers fare differently due to the volume asymmetry. Consider that most consumers only experience one or two problems with their eCommerce purchases in a given year, and rarely (if ever) do consumers experience problems with the same merchant. That means that even if a consumer experiences multiple purchase problems, it is likely that the consumer will have to navigate different complaints processes for each store or merchant. They may call some companies seeking remedies, file claims with ODR systems where possible, write emails to other companies, etc. Consumers therefore gain no repeat player advantages with any one complaint system.

Amy J. Schmitz *is the Elwood L. Thomas Missouri Endowed Professor of Law at the University of Missouri-Columbia School of Law.* *I thank Colin Rule for his collaboration on ODR projects over the years, which contributed greatly to this essay that is adapted from concepts in our book, Amy J. Schmitz & Colin Rule, THE NEW HANDSHAKE: ONLINE DISPUTE RESOLUTION AND THE FUTURE OF CONSUMER PROTECTION (2017). I also thank Rachel Mitchell for her comments.*

In contrast, sellers experience problems on approximately 1 to 3 percent of their overall sales volume. If a seller sells 100 items a month, that means 12 to 36 disputes a year. If they sell 1000 items a month, that is 120 to 360 disputes a year. As sales volume increases, so do disputes. This volume asymmetry gives the seller a significant advantage. Sellers are the proverbial "repeat player." The merchants learn the system, and can afford to hire the requisite legal assistance to help them navigate complaints toward their favor.

This relates to the information asymmetry. The seller (or the customer service employees working for the seller) quickly develops a lot of expertise about how the resolution process works. Sellers know what policies govern the outcomes rendered by the process, and they know what evidence will likely sway a decisionmaker. The consumer likely enters the process with no awareness of how it works, while the merchant enters the process with a long track record of lessons learned. That also means that the consumer must learn the rules as they navigate the process, while the seller already knows how everything is going to proceed.

The third asymmetry is the resource asymmetry. Sellers have the resources to support a long and extended resolution process, while consumers do not. Sellers also have the funds to retain counsel to deal with larger claims, and to apply policies for "paying off" the squeaky wheels, or highly valued consumers due to their zip codes or history for large purchases. However, such policies may harm those with the lowest incomes—essentially the consumer "have-nots."[3] These consumers are on their own in navigating remedy processes and seeking any sort of relief. That means that a well-designed and fair redress process must be built for any user, regardless of education or resources. It must require no legal representation, understanding of policies and precedents, or presentation of evidence.

Accordingly, there is danger that volume, information and resource asymmetries will converge to tilt any ODR processes to favor merchants. However, we can design a resolution process that simultaneously compensates for the repeat player advantage and the three types of asymmetry. The solution is to give consumers control, while providing extensive help content and algorithmic support to counteract the information asymmetry that sellers enjoy. Control comes from simplicity. Consumers gain a sense of empowerment and control when they can easily navigate a resolution process without need for legal assistance or advanced education. In other words, online consumer redress processes must be very simple and straightforward for the consumer so that consumers are not disadvantaged by their lack of prior experience.

Furthermore, algorithmic support addresses the information asymmetry by digesting data from prior cases and complaints, and suggesting fair resolutions. A well designed ODR system must therefore leverage information drawn from the experiences of thousands of other buyers. Armed with data regarding prior cases and resolutions, consumers will not be left "in the dark" navigating their way toward a resolution. Furthermore, system monitoring and external auditing of the ODR process and any algorithms used should be added to catch repeat player problems when they arise. Indeed, it is easier to test ODR fairness than traditional processes due to the ease of system data collection and use of data auditing techniques.

SETTING A DOLLAR LIMIT

One of the major debates regarding UNCITRAL Working Group III on ODR focused on the intended scope of a global ODR system and the definition of Business-to-Consumer (B2C) verses Business-to-Business (B2B) cases. Determing whether a buyer is a consumer or a buisness is not a simple matter. Some businesses go online to buy large amounts of goods to stock their brick-and-mortar stores, while other sole proprietors make very few small dollar purchases and feel like "little guys" in eCommerce. It also is difficult to tell whether a seller is a professional or a hobbyist. If a seller is posting homemade mittens out of her kitchen, is she a consumer or a professional seller? At what point does one switch from being a consumer to being a merchant, and should it matter for determining the scope of a global ODR system?

Accordingly, it seems wise to bypass the debate regarding what qualifies as a "business" to define scope for a global ODR system. Instead, the best way to handle the issue is to simply set a dollar limit for the system, and include all transactions under that limit regardless of whether one would view them as B2C or B2B. This value may be different in different

geographies, and it will change over time. Of course, the meaning of "low value" claims comes with its own difficulties, but it is much easier to tackle. It is nonetheless possible to set an amount, such as $1,000 and other currency equivalents, as a starting point. The amount could rise to $5,000 and currency equivalents, as $5,000 often is used for small claims courts in the United States. This would be a better starting point than getting hung up on the question of how to effectively triage cases into B2C and B2B buckets.

BYPASSING THE BINDING VS. NON-BINDING DEBATE

The question of whether ODR systems should deliver binding outcomes has complicated many of the discussions around consumer redress. Indeed, dissention remains regarding the legitimacy of any binding ODR for resolution of B2C claims. There are strong arguments for evaluative approaches: Evaluative outcomes can provide 100 percent closure and can be extremely efficient to deliver at volume. Some parties also desire an evaluative determination in order to know whether they are "right." Furthermore, parties gain assured access to remedies from final determinations. This gives disputants an incentive to put forth all their evidence, not holding facts back for future litigation, as may occur in non-binding facilitative processes.

That said, policymakers, scholars, and consumer representatives have criticized binding arbitration in face-to-face consumer processes. They argue that pre-dispute binding arbitration clauses undermine valid consent and the enforcement of statutory consumer protections and other public rights. Many legal jurisdictions in Europe, for example, forbid the use of pre-dispute binding arbitration clauses in consumer transactions. They often reserve evaluative decision making only for public bodies, such as Ombuds Offices or Consumer Courts. In these geographies, it would not be legal to require ODR outcomes to be binding on consumers.

It should be noted that there are ways to deliver evaluative outcomes in a manner that abides by due process and fairness standards. For example, increasing transparency and adding external audits assist fairness of binding processes. Evaluative determinations could be published on a central portal after appropriate redaction of private information. This portal could be easily searchable, and allow consumers and consumer advocates to learn about recently resolved cases. Although some companies may be uncomfortable with such transparency, others would welcome opportunity to garner goodwill and competitive differentiation by complying with consumer protections and providing remedies to deserving consumers.

Ultimately, however, consumers should have free choice. They should not be compelled to abide by a binding private resolution without full information to weigh the benefits and costs. Consumers should retain the right to seek public redress. Therefore, ODR systems should not block access to the courts for consumers. But if the systems are well designed, they will resolve 99.99 percent of consumer cases without need for judicial redress. Moreover, the process would expand access to any remedies, since most low dollar consumer claims would never go to court anyway. Consumers often are simply left with no recourse because the costs of pursuing claims outweigh any likely redress. A free or cheap ODR process would therefore open avenues to remedies, and advance consumer protection.

DEALING WITH MASS CLAIMS

Isolating claims in private redress systems prevents the public from learning about major consumer protection issues. That is a major criticism of arbitration as it currently operates. If every matter is viewed as a single case, the onus always is on the complainant to report the incident in order to get their particular situation addressed. Complainants often do not have the full picture, as they only know their particular experience. This makes it very difficult to connect the dots to identify more systemic problems.

Advocates for mass claim processes such as class actions argue that resolution processes that require each aggrieved consumer to file an individual case will inevitably under-report problems because some percentage of consumers will not bother to report their issues. This means that the full extent of the situation will not be remedied. Class actions, they argue, are the only means for bringing justice to individuals with low dollar claims and shedding light on the full scope of the problem to be resolved.

These criticisms have merit, and class actions can be very powerful. Effective ODR design, however, can address transparency and allow for new means of consumer protection without the costs and drawbacks of class actions. One potential approach can be drawn from Consumer Ombuds offices in the European Union. European countries do not have class actions as we do in the United States; but they are committed to providing strong consumer protection. A global ODR system can borrow from their design by including a tripwire-like mechanism. The tripwire is triggered when a certain number of cases are filed that fit the same fact pattern.

To some extent, this is happening in the United States with the Consumer Financial Protection Bureau (CFPB). As consumers report issues in the CFPB's complaint portal, staffers with the CFPB look for patterns in the reports. If enough similar reports are filed, the tripwire is activated, and the CFPB will notify the business and require them to do an investigation to see how many consumers might have been similarly affected.

It would be very easy to build in such a tripwire for a global ODR system. Resolutions always should start at the individual case level, but effective data collection can enable pattern detection algorithms that make it easier to detect more systemic issues. Some companies may dislike this idea, as it allows regulators to "catch" bad actors, but companies should embrace this idea. It would allow them to learn of issues before they escalate into costly class claims. Moreover, the "good guys" benefit when the regulators and consumers become aware of the "bad guy" practices and products. Next generation consumer redress systems must therefore provide resolutions that scale from single issues to mass claims within the same platform if they are to be truly effective.

BUILDING AN ODR TRUSTMARK

Merchant and sales platforms have been designed to rely heavily on seals or badges to indicate that a merchant is a trustworthy and reliable transaction partner. In many environments, these trustmarks, such as the Better Business Bureau "BBB" seal, or the TRUSTe logo, are a valuable tool for businesses looking to establish their legitimacy online. When an eCommerce merchant first enters a market or region, the consumers in that region may have no idea whether it is trustworthy. Trustmarks, particularly those issued by a well-respected organization or public agency, can help new customers feel that merchant is safe and competent.

Trustmarks are especially important for new merchants in providing consumers with some means to trust and make purchases. New merchants do not have ratings or track records. Accordingly, it would help consumers to feel comfortable buying from new or smaller vendors if these vendors have earned the right to post an ODR trustmark that signifies the vendor's commitment to an ODR protocol for providing a fair redress mechanism for consumers to obtain remedies if purchases go awry. Furthermore, this trustmark would go beyond unmonitored review sites and clear a way toward justice in eCommerce.

That is not to say all trustmarks have value. It can be extremely difficult for the organizations that issue the trustmarks to manually monitor the behavior of all of the organizations who have opted into the trustmark program. Even the BBB has been criticized for not sufficiently monitoring businesses under its seal. In addition, other organizations may create fake or less stringent trustmarks, thereby impairing the value of all trustmarks and causing confusion as to which trustmarks are trustworthy. Eventually trustmarks lose meaning and consumers no longer care about their existence when deciding where and how to make purchases.

At the same time, some argue that trustmarks are unnecessary due to review sites such as Yelp and TripAdvisor, and purchaser reviews on merchant sites such as Amazon. The argument is that because these sites aggregate information from thousands of users, the four or five star rating of a merchant can be trusted as a good indicator of their reliability. The problem is that these sites also have lost credibility due to "flogging," or posting fake blogs and reviews lauding products and services. Merchants also hire individuals to post fake reviews touting their own businesses and/or criticizing competitors. Furthermore, these reviews generally are unmonitored and their veracity is suspect. Deciphering reviews also is difficult because they rely on the subjective thoughts of the poster. This makes reviews a poor stand-in for more thorough external performance auditing, leaving consumers even more vulnerable to misleading information and bad experiences.

Accordingly, a well-conceived and monitored trustmark system would be beneficial for building an ODR system. There could be one unifying trustmark that earns respect through proper creation. Private entities could work in collaboration with government regulators and other external auditors to ensure that the trustmark system is ethically administered. Specifically, merchants would earn the right to post the trustmark by agreeing to follow prescribed ODR standards of speed, fairness, and accountability. A public/private consortium would then monitor the system. A certain amount of this work could be done digitally with algorithms that catch patterns or lack of response, but there also would be some costs from human monitoring. Small subscription fees could help cover these costs.

SYNTHESIZING DESIGN CRITERIA

The challenge now is to take these observations and distill them into a plan of action. The following is a nutshell meant to catalyze discussion and development.[4] Indeed, the time is ripe to bring global ODR to fruition.

FAST, FREE AND FAIR

First and foremost, we know that consumers want fast and easy resolutions. Individuals have no desire or time to pick up the phone and wait on hold or waste time haggling over a fair solution. Consumers have endured that pain for far too long. Consumers also will run from any fees for using a process for simply getting what they were promised. ODR, therefore, must be simple to access, free to consumers, and easy to understand.

This also means that the initiation for the process should reside in exactly the same location where the transaction originally took place: on the merchant's Web site. The consumer should be easily able to report an issue, and should get a solution as quickly as possible. Instant determinations would be best; failing that, however, a resolution in hours or days instead of weeks or months.

Online guides and wizards should be available to enable consumers to easily educate themselves about their rights, evidentiary obligations, procedural steps, and likely outcomes. Consumers must know exactly what they are getting into when they initiate the process. They must never feel surprised or misled by a procedural development that they did not know about prior to filing the case.

Furthermore, consumers using the system should not fear retribution for filing a claim. Data collected should be scrubbed of personally identifying information, and merchants should be prohibited from "punishing" consumers for filing to seek redress. The consumers that will use this process are likely to feel that they have been treated unfairly once, and that is the reason why they decided to try ODR. We must do everything in our power to ensure that they do not feel doubly mistreated by this redress design, and that it is as easy and straightforward as it can be, in order to ensure the consumer feels the process was fast and fair.

HIGHLY SCALABLE

This global ODR system should not simply benefit consumers. It also must benefit merchants or they will never "sign on" and adopt the system. Scalability is therefore a must. Scalability makes ODR a problem-solver for merchants across the globe.

Merchants face an incredible volume of disputes through eCommerce (projected to be more than 1 billion disputes per year in 2017 and beyond). This volume of disputes simply cannot be resolved through human powered resolution procedures. It is much too expensive for merchants to hire sufficient customer service representatives and lawyers to deal with all the disputes eCommerce generates. This makes algorithms incredibly effective and efficient for resolving eCommerce disputes. For example, algorithms using data regarding similar disputes could help generate quick remedies and settlements.

Critics of algorithms argue that computers should never decide disputes because they eliminate the compassion and empathy of in-person interactions. However, that ignores the fact eCommerce is generated online and over the Internet—by and through computers. Most, if not all, purchasers and merchants over the Internet do not care about personal connections. They simply want swift transactions and remedies when purchases go wrong. Algorithms that are

carefully constructed and closely monitored have the power to provide the type of fast and fair resolutions consumers crave.

That said, not every case can be effectively resolved by algorithm. The ODR system must work like a filter, where algorithmic resolutions handle the easily resolvable cases. This would leave a much smaller volume that requires human attention. That means that algorithms will use data to suggest settlements, thereby leading to resolutions of nearly all cases. Nonetheless, online mediators and arbitrators could handle the few cases left unresolved. Telephone and in-person assistance also could be available as a last resort.

This approach is the only way to make the system sustainable. Consider that most eCommerce purchases are under $100. It is very hard to imagine a human-powered resolution process that will be able to handle cases at that price point on a cost-effective basis. Companies would have to spend exponential amounts to build up customer service, along with an abundance of mediators and arbitrators to resolve all of these claims. An ODR process that handles most issues through algorithms would therefore save companies costs in dealing with complaints. Moreover, such ODR would be built to scale, thus helping solve the customer service problem and assisting merchants to retain happy and loyal customers.

SECURE

The daily news is filled with stories of scams and data privacy disasters. Consumers nonetheless are eager to continue making purchases online. In the process, however, they want to be sure that their privacy is respected. Consumers want to receive exactly what they were told they were going to get when they agreed to the transaction, and they do not want to be stuck with things without consent. They certainly do not want to learn that their data has been sold and used in improper ways.

This brings in security and privacy. Part of being treated with respect is a commitment to maintaining consumer privacy. Consumers know that businesses are tracking when they make online purchases, use store loyalty cards, or pay for goods or services using their credit and debit cards. Data brokers track spending habits, how long one lingers on a Web site, consumers' online searching histories, family information, and even postings on social sites such as Facebook. Consumers may tolerate this data collection if it is used to improve their shopping experience, but they are intolerant of businesses treating their private data like another product to be bought and sold.

This is especially true when seeking remedies and settlement. A global ODR process must therefore respect privacy and preclude any sale of collected data. Some data about claims and issues may be collected, but it only should be used *to improve the process and assist in predicting proper remedies* based on similar cases. Again, that data must be scrubbed of personally identifying information. Moreover, data security must be a central component of the system. The ODR platform must be encrypted—and certainly much safer than email.

AMICABLY TONED

Tone is incredibly important. A global ODR system must set the right tone or it will fail at the outset. This is especially true given the variety of cultures and backgrounds of its users. Therefore, systems built under the presumption that all reported issues are fraud will generate frustration and inspire claims. The data shows that problems are inevitable, and the majority of them are resolvable through direct communication. Consumers and merchants want to have successful transactions, and they can be trusted to do the right thing most of the time.

This means that an ODR system should provide guided communication flows that provide a proper mindset. If the language used within a redress flow presumes ill intent (*e.g.*, filing a "fraud alert" instead of "reporting a problem") then the users within that system similarly will assume that the other side is a bad actor that needs to be punished. The better approach is to provide simple flows starting with "item not received" or "item not as promised." Factual flows from these basic starting points keep the communications focused on finding a solution in good faith.

Ultimately, it is best when consumers and merchants can resolve a matter through mutual

agreement and direct communication. That is the best outcome for a reported problem. This brings us back to the binding/non-binding debate regarding arbitration noted above. When evaluative systems impose a punitive, victim-offender narrative on problems at the outset, one party always will leave the case feeling frustrated. Accordingly, ODR guided flows focused on facts and not judgment lead to the highest satisfaction.

CONSISTENT

An immediate concern regarding ODR is that it eventually will skew toward the repeat players, as noted above. Of course, as soon as a redress system is launched, potential users immediately test it. They may generate a barrage of cases and try out the different scenarios to see if they can find a seam in the design that they can exploit. Consider the individual who continually tries different scenarios in Turbotax hoping to lower one's taxes.

Accordingly, it is of utmost importance that the global ODR system be designed to combat this type of gaming. When vulnerabilities or perverse incentives are discovered in the flow, they must be addressed quickly. As the system matures, and designers re-code, reconsider, and redraft policies, new opportunities emerge for the delicate power balance between participants to be negatively affected. This is especially problematic when the profit motive comes into play. Good intentions at launch can come unstuck over the years if the systems administrators pay too much attention to maximizing the revenue stream. This is a challenge for all redress systems, public or private, but private interests may be even more susceptible.

That is not to say that private companies should not play a vital role in creating ODR processes. Indeed, they are essential because only they are able to stay abreast of rapidly evolving developments in technology and the global eCommerce marketplace. But independent evaluators should play a role in ensuring the fairness of these privately created processes.

This can begin with tripwires that notify public regulators and non-profit oversight organizations not only of large volumes of claims regarding the same products, but also when it appears that outcomes have become skewed. Once filings cross the specified threshold or indicate that outcomes may be skewed to favor a certain merchant, regulators may be automatically notified of possible grounds for an investigation or enforcement action. Also, these tripwires may result in an automatic public notification to inform other consumers of a potential recurring problem. This type of automated action could be important especially to catch "gamers" and to alert the public of health or safety issues are at stake.

These automated notification systems also could ease companies' overall dispute resolution costs by making the entire redress process more cost effective and efficient. The trust benefit obtained by participating businesses would provide more than enough economic benefit to justify participation. Furthermore, companies' participation in the ODR process should help them avoid any potential enforcement actions and class claims, and the courts should view participation in externally audited third party resolution systems as a strong signal that companies are committed to treating their customers fairly.

BENEFICIAL TRUSTMARK

As noted above, building a trustmark for ODR could be beneficial to companies and consumers. This trustmark should (a) communicate to buyers that this system is a safe and effective place for them to resolve purchase problems; (b) earn positive notoriety to set it apart from the morass of other redress schemes promoted across the Internet; and (c) be cross-culturally valid and appropriate in a wide variety of geographies.

Ideally the trustmark should create an affiliative halo from participation if respected public and private entities contribute their reputations to the administration and management of the system. Quality merchants will be eager to associate themselves with leading consumer protection and advocacy organizations, even if participation does generate additional responsibilities. The goal is to build a reliable resolution process that consumers will come to understand and utilize, and businesses will realize a trust benefit from their participation.

Such an ODR trustmark should not be a goal in itself. Instead, it should be valuable to both

consumers and merchants. It should be the backbone of a new ODR opt-in mechanism to provide buyers a tool that they can utilize should a purchase go wrong. At the same time, it should give merchants credibility, and help them obtain and retain loyal customers. Accordingly, the program must include mechanisms to throw out underperforming merchants from the program. The credibility of the system is dependent on strict enforcement of the merchant guidelines. If businesses repeatedly flout the rules and do not resolve buyer complaints, yet remain in the system, the trustworthiness of the overall program may be irreparably damaged.

ENFORCEABLE

Any ODR system that leaves merchants free to ignore resolutions is useless. Currently, some online marketplaces have not done the work required to enable effective enforcement of outcomes. For example, some classified sites do not enable buyers and sellers to hold their transaction partners accountable for performance once the transaction is complete. Users may have no fixed username or account, and no concrete way of getting a remedy once payment is made. The consumer may know nothing tangible about the merchant, and may be unable to contact them with any questions or problems.

For example, if an online marketplace provides only a disposable forwarding email address for a transaction partner, and the parties make a cash deal in person, there is no way to resolve a later problem. Consider the buyer who pays $500 in cash for a laptop, meeting the seller in a parking lot, and then later discovers the laptop is completely non-functional. The buyer has no way to contact the seller to ask a question, and there is no way to reverse the payment made in cash.

In contrast, an ODR system must be built to allow for tracking and enforcement. Delivering resolutions to consumers that must then find ways to enforce is not an effective design. Enforcement should be automated, effective, and integrated into the transaction from inception. Merchant contacts must be tested and tracking must be part of the ODR system. Furthermore, merchants who fail to abide by resolutions and settlements must lose ability to post the trustmark. Ultimately, they must be eliminated from the program, thus harming their ability to gather and retain customers.

ADAPTABLE

One of the key attributes of ODR is its adaptability. Any computer coder or software designer will tell you that no solution is perfect on the first try. No matter how much research, planning, and testing one does in advance of bringing a system live, adjustments always are required. Furthermore, regardless of whether a system seems to be working at launch, conditions always are changing, which requires any platform to be able to evolve and adjust if it is to remain effective over the longer term.

A global ODR system must therefore be ready to adapt and change. This will be fueled by scalability, and the high volume caseloads in eCommerce disputes. The system itself will generate a lot of data, and effective systems designers will then be able to analyze the data to learn from that flow and continuously improve the system over time. ODR systems also have the advantage of being able to engage problems much earlier in the lifecycle of the issue, and early resolutions are the most effective. ODR systems also can offer valuable insights upstream of disputes, so that the transaction environment itself may be able to adjust to prevent later misunderstandings that can turn into problems and disputes. This discipline of continuous improvement and learning should be integrated into the ODR system's design from inception to ensure continued relevance and effectiveness.

CONCLUSION

It is not simple to design and build a global ODR system that can handle high volumes, cross cultures, and continuously improve. Key debates around asymmetries, scope, consent, class claims, and trust have stymied development of such a system since UNCITRAL Working Group III ended in 2016. These debates, however, can be addressed. There are ways to design an ODR system that will be effective over the long term. This article aimed to crystalize key considerations and lay out design criteria to create a foundation for this system. The challenge now is to engage private and public entities to take the lead

and work with merchants and consumers on a global level to take these observations and craft a systems design that integrates them into an implementable ODR solution for global eCommerce claims.

NOTES

1. Consumer Financial Protection Bureau, Final Rule, Arbitration, Nov. 1, 2017, at *https://www.consumerfinance.gov/policy-compliance/rulemaking/final-rules/arbitration-agreements*. On Nov. 1, 2017, the President signed a joint resolution passed by Congress disapproving the Arbitration Agreements Rule under the Congressional Review Act (CRA). This essentially overturned the CFPB's proposed rule that would have precluded enforcement of predispute arbitration clauses in consumer financial product and service agreements where it would hinder class actions.
2. *See generally,* Amy J. Schmitz & Colin Rule, The New Handshake: Online Dispute Resolution And The Future Of Consumer Protection (2017). Again, the ideas in this essay are further distilled and explored in this book.
3. Amy J. Schmitz, Secret Consumer Scores and Segmentations: Separating Consumer "Haves" from "Have-Nots," 2014 *Mich. St. L. Rev.* 1411-1473 (2015).
4. These ideas are further explored in my book with Colin Rule, *supra* n.2.

The Right to Data Portability from page 1

INTRODUCTION[3]

On January 25, 2012, the European Commission (the Commission) proposed a reform of the EU's data protection rules by drafting the General Data Protection Regulation (GDPR) in order to strengthen online data protection rights and boost Europe's digital economy. It was also done to adapt to technological advancements that had taken place in the previous decade, following the introduction of the Data Protection Directive.[4] While the provisions of the GDPR build upon those established under the Data Protection Directive, the rules under the GDPR are more stringent[5] and hold a wider scope.[6] The reactions to the GDPR have been mixed. Some scholars[7] saw it as a welcome development, however others[8] have raised concerns.

The right to data portability in the GDPR will require businesses to ensure that they can hand over personal data provided by an individual[9] in a usable and transferable format. The preamble of the GDPR demonstrates that the right to data portability will be applicable to cloud computing, Web services, smartphone systems and other automated data processing systems.[10] The right to data portability will apply to a wide range of areas such as social media, search engines, photo storage, email and online shops. It will be equally applicable to banks, pharmaceutical companies, energy providers, airlines—even small businesses such as pizza shops or tailors if they are data controllers and deal with personal data.

The final text of the GDPR was agreed to in the trilogue between the European Council, Parliament and Commission on December 15, 2015, and published on May 4, 2016 in the Official Journal of the European Union.[11] After a two-year transition period, the GDPR will be binding on all member states from May 25, 2018.

The right to data portability is contained under Article 20 of the GDPR. It can be seen as an extension of an individual's right of access under Article 15 of the GDPR.[12] It has two key elements: (1) the right of the data subject to obtain a copy of personal data from the data controller; and (2) the right to transfer that data from one data controller to another. The text of the GDPR arguably limits the scope of the right to data portability and contained some ambiguities. Following an open public consultation, which ran through the end of January 2017, on April 5, 2017, the Article 29 Working Party[13] approved a revised and substantive guidance (hereinafter referred to as the 2017 revised guidelines on data portability) clarifying some of the ambiguities with regards to the right to data portability.[14]

This article examines the right to data portability under the GDPR to establish whether any lessons can be drawn from the EU experience, particularly for the United States. This article critically analyzes the issues raised by Article 20 of the GDPR and potential enforcement problems. It also gives an overview of the state of data portability in the United States and provides lessons to be learned from the EU experience.

CRITICAL REVIEW OF THE RIGHT TO DATA PORTABILITY—KEY ISSUES IN THE GDPR[15]

LIMITATIONS ON DATA GENERATED BY THE DATA CONTROLLER

Article 20 of the GDPR only applies to data provided by the data subject. The Article 29 Working Party published a summary of discussions that took place at the Fablab Workshop July 26, 2016.[16] It gave a good overview of key issues in relation to data portability.

In the context of data portability, Article 29 Working Party highlighted the importance of clarifying what is meant by data that has been provided by the data subject, as a narrow interpretation of personal data would result in fewer benefits for individuals while a very wide interpretation of it would be a concern for data controllers.[17]

As mentioned by Graef et al, the wording of Article 20 of the GDPR does not clarify whether the data that has been generated by the service provider for statistical and analytical purposes, such as online reputations, could be subject to data portability or not.[18]

As pointed out by Graef et al,[19] in an auction Web site such as eBay the contact information and the advertisements are provided by the seller (data subject) himself but the provider adds feedback

scores to the seller's profile and these form part of the reputation that a seller has built on. Hence, a literal interpretation of the adopted text would only allow the users to move their personal information to another auction site while not being able to move their ratings and reputation to another auction site as the latter is provided by the service provider. For an online user it is crucial to show that he/she has built a good reputation when he/she moves on to a different platform. Without moving this reputation, it is highly unlikely that the seller would attract new buyers in a new platform. Ultimately, this can hinder users from moving to another platform.

The April 2017 revised guidelines on the right to data portability offer some helpful clarification with regards to the above-mentioned ambiguity by stipulating that data provided by the individual should include "the personal data that are observed from the activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of Web site usage or search activities."[20] In other words, according to the revised guidelines on the right to data portability the term provided by data subject includes the data that result from the observation of an individuals' behavior but it does not cover 'inferred' data resulting from the subsequent analysis of that behavior by the data controller.[21] Hence it could be said that Article 29 Working Party takes a broader interpretation of personal data, which is a welcome interpretation in terms of extending the scope of data portability in the EU member states.

In the context of Graeff's example, buyer/seller ratings on eBay would fall within the scope of observed data, which would be portable from one controller to another, while an average of these scores calculated by the data controller (processor), would not.

The Article 29 Working Party also clarifies that meta data that is needed to meet the data subjects' objective, to move data from one service to another, falls within the scope of Article 20 of the GDPR.[22] As an example, the right to data portability would require a data controller to not only transfer the emails sent and received by the data subject but also other relevant information such as timestamp information and other information showing whether emails have been read or not.

The clarifications in the revised guidelines on data portability go a long way in meeting the need for clarification. Nevertheless, it will be interesting to see whether data controllers will find ways of circumventing the revised guidelines in order to refuse to transfer data to another controller and it will be important to monitor any potential problems in order to address them in the future.

PRIVACY RIGHTS OF THIRD PARTIES

Another limitation of the right to data portability concerns the privacy rights of third parties. As noted by Engels, allowing one user to transfer a second user's information to another platform may violate the privacy rights of a second user.[23] For example, when several people appear in a photograph on Facebook, even if one data subject wants to import it to another social networking platform, this cannot be done, as it would impact privacy and data portability rights of other individuals appearing in that picture. Another example is a bank transfer with information pertaining to both buyer and seller. This implication seems to have been taken into account by the legislators as paragraph 4 of Article 20 GDPR states that the right to data shall not adversely affect the rights and freedoms of others.

The revised guidelines by the Article 29 Working Party make it clear that even if the requested data might have an impact on the privacy rights of third parties this does not stop it from being transferred to another controller.

Their proposed solution to deal with potential shortcomings is two–pronged. First, "The processing operations initiated by the data subject in the context of personal activity that concern and potentially impact third parties remain under his or her responsibility, to the extent that such processing is not, in any manner, decided by the data controller."[24] In other words, according to the April 2017 Guidelines on the right to data portability, if the data relates to the person making the request as well as third parties, it is the responsibility of the person making the request to ensure that data protection right of third parties are respected.

Second, the revised guidance asserts that "the rights and freedoms of third parties will not be respected if the new data controller uses their personal data for purposes other than to deliver a service to the data subject who has ported the data.[25]" For instance,

if the new data controller uses the data of third parties for direct marketing purposes, it would be contrary to the revised guidelines on data portability.

TECHNICAL FEASIBILITY OF DATA TRANSFER

A significant challenge for the enforcement of the right to data portability concerns the "technical feasibility" sought for the data portability across the platforms. Arguably, what is technically feasible for one data controller might not be technically feasible for another data controller. Given the wording of Article 20(2) of the GDPR it is likely that some data controllers will contend that such a transfer is technically infeasible. As a result of this wording the transfer of data may be undermined and overlooked by data controllers. As there is no reference to the Commission's authority to specify the electronic format necessary for data portability in the GDPR, collaboration among market players is crucial in devising industry norms and standards.

In its revised guidelines issued on April 2017, the Article 29 Working Party offers valuable clarification with regards to the notion of technical feasibility and controller to controller transfer.

Article 29 Working Party states that "where no formats are in common use for a given industry or given context, data controllers should provide personal data using commonly used open formats (*e.g.*, XML, JSON, CSV) along with useful metadata at the best possible level of granularity**,** while maintaining a high level of abstraction."[26]

As regards "technically feasible" Article 29 Working Party holds that "… direct transmission from one data controller to another could … occur when communication between two systems is possible, in a secured way, and when the receiving system is technically in a position to receive the incoming data."[27] This can be interpreted as there being no impediment to invest in new functionality where existing systems do not support controller-to-controller transfer.

In terms of enforcing direct controller-to-controller portability it seems that the Article 29 Working Party has chosen to rely on two mechanisms to motivate direct transfer: (1) data subject pressure by empowering data subjects to demand an explanation as to why data controllers are unable to offer direct controller-to-controller portability;[28] and (2) the administrative burden of repetitive data subject requests, where data subjects can be expected to demand usable data vis-à-vis a range of disparate systems.[29]

Whether the pressure from data subjects to ensure direct controller-to-controller portability will prove effective, remains to be seen. It will be interesting to see whether data controllers will come up with ways to circumvent data portability by suggesting that such transfer is not technically feasible, when it is in fact possible.

A stricter requirement for direct controller-to-controller transfer could still turn out to be a necessity, one that in a few years with open Web technologies will seem both more reasonable and more feasible.

DISPROPORTIONATE COSTS AND EFFORTS

Forcing data controllers to transfer personal data may result in disproportionate costs and efforts.

Article 20 of the GDPR requires an online service to write specialized code—export-import module (EIM)—that will export data from that service and import it to another service. As noted by Swire and Lagos, many small and medium-sized companies do not have the resources to fully understand the GDPR, comply with it and write an EIM to move data to another provider.[30]

Neither the Commission nor other EU institutions have presented any figures as to the cost of complying with data portability requests. According to a study by Christensen *et al,* the GDPR reform would increase European small and medium-sized enterprises' annual IT costs by between approximately € 3.000 and € 7.200 depending on the industry the particular SME is operating in, representing between 16 and 40 percent of their yearly average IT budgets.[31] It is not clear what percentage of this budget will be spent responding to data portability requests.

Swire and Lagos also support this point and argue that the GDPR would impose substantial costs on suppliers of software and apps.[32]

While such costs may not be significant for large companies, the requirement is likely to create problems for small and medium-sized companies. It must

be noted that complying with the GDPR should not to be taken lightly due to the heavy fines associated with failing to do so. According to Article 83(5) of the GDPR, a data controller that fails to comply with data portability provisions in the GDPR will incur administrative fines up to 20 million EUR or in case of an undertaking up to 4 percent of the total worldwide annual turnover of the preceding year, whichever is greater.

The issue of disproportionate costs also was raised in December 2015 by Baroness Neville Rolfe, the United Kingdom's parliamentary Under-Secretary of State for the Department for Business, Innovation and Skills. She stated that data portability rules designed to enable consumers to move their data from one platform to another should not be too costly as they can serve as an entry barrier into markets, and this might have an adverse effect on innovation and competition.[33]

The Article 29 Working Party, however, does make it clear in the guidelines that the role of being data controller in the European Union moving forward should be considered a normal cost of doing business along the lines of accounting, insurance, and other unavoidable costs. The Article 29 Working Party explicitly holds that the overall system implementation costs cannot "be used to justify a refusal to answer portability requests."[34] Time will show whether dealing with data portability requests will be too costly for businesses or whether these costs could be seen as an ordinary cost of running a business as suggested by the Working Party.

PROPRIETARY INFORMATION AND INTELLECTUAL PROPERTY RIGHTS

If the personal data that needs to be transferred contains valuable proprietary information and intellectual property, this might discourage companies/service providers from creating the proprietary information in the first place.

The case of True Fit,[35] an online digital service helping users of online clothing retailers such as House of Fraser to find the right cloth sizes for their shoppers, illustrates this point. The True Fit service asks shoppers to share a wide range of personal data such as height, weight, measurements, body type, and information such as what brand and size their favorite clothing comes from. Users share this information with True Fit, which then shares it with online retailers. Arguably, if True Fit were to be required under the data portability provision to transfer this data to other retailers, its business model would become obsolete.

Recital 63 of the GDPR provides that the general right of access under Article 15 could be restricted if it adversely affects the rights and freedoms of others, including trade secrets and intellectual property rights. As the right to data portability can be seen as an extension of the right of access, arguably the limitation mentioned in Recital 63 should be applicable in the context of data portability requests. In other words, when faced with data portability requests companies, data controllers should be able to strip valuable data from the dataset if it adversely affects trade secrets and intellectual property.

Nevertheless, neither recital 68 of the GDPR pertaining to the limitations of the right to data portability, nor Article 20 of the GDPR specifically suggests that the right to data portability can be limited if it adversely affects trade secrets and intellectual property. Hence there was a need for further clarification as to whether the right to data portability might be restricted when it affects proprietary information and intellectual property rights.

If companies, such as True Fit, stop creating valuable services based on personal data, clearly this will have a stifling effect on innovation and consumer welfare. This would, ultimately, have an adverse effect on consumers who would be deprived of choice and useful products.

In the revised guidelines on the right to data portability, the Article 29 Working Party provides some guidance with respect to the above and holds that "The right to data portability is not a right for an individual to misuse the information in a way that could be qualified as an unfair practice or that would constitute a violation of intellectual property rights."[36] Furthermore in its guidance the Article 29 Working Party suggests that data controllers can provide the information requested in a form that does not release information covered by trade secrets and intellectual property rights.[37] However it must be noted that this might not be always easy to implement. Hence there is definitely need for further guidance on this issue.

As seen above in the discussion of privacy rights of third parties, the Article 29 Working Party guidelines on data portability fail to offer protections for

current data controllers, while making it clear that the data subject, and the receiving data controller has every right to request data when the purpose is to provide a service to the data subject, regardless of the impact on the current data controller.

In light of the above, it is unclear whether a third party data controller such as True Fit will be able to stop competitors, or current customers, from receiving information and use their service for free. Time will show if such firms and services will potentially suffer due to business models seemingly at odds with the GDPR, and what the cost of that will be to consumers and to the economy.

ENFORCEMENT ISSUES PERTAINING TO THE RIGHT TO DATA PORTABILITY

The main objective of the right to data portability is to empower consumers so that they can get a copy of their electronic personal data, demand transmission of their personal data to another provider and switch to other providers.[38] Hence, the objective of the right to data portability overlaps with the objectives of other areas of law, *e.g.*, competition law, consumer protection laws, and so forth.

Similar to other data subject rights in the GDPR, data portability is a right, which needs to be invoked by the data subject and cannot be relied on by parties such as small and medium sized businesses. For instance, a small business cannot demand data portability from its business bank but an individual can. This raises some problems regarding its legal and theoretical boundaries, as well as enforcement within the realm enshrined by the GDPR.

Furthermore, there is no clarity as to whether users will make use of the right to data portability. In order to ensure that data subjects invoke the right effectively, data subjects need to be informed as to what this right entails.

Hence, Article 29 Working Party should liaise with national data protection agencies in order to make sure the necessary investments are made in educating the public about their rights. As a minimum, national data protection agencies should have information on their Web sites in plain and simple language explaining to users how they can approach the data controller for data portability requests and advise them on how to make a complaint if the data controller refuses to provide the data. Making a complaint must be easy and the data subjects should not incur substantial costs or risks as this might discourage them from exercising their rights.

Furthermore, while the Article 29 Working Party guidelines do not refer to enhancing competition between services as an objective of data portability, several authors[39] have suggested that competition law and provisions may contribute to the enforcement of data portability legislation, in particular where the data controller is a dominant actor in a monopolistic market applying unfair restrictions on data portability. In this context, failure to offer direct controller-to-controller data portability without a valid and sensible reason could be seen as an abuse of a dominant position (or monopolization in the US context) and potentially be remedied by competition/antitrust laws.

PRIVACY AND DATA SECURITY RISKS

Security and privacy concerns arise when data is transferred from one data controller to another. Data can end up in the wrong hands if access is granted to the wrong person—an investigator making a pretext call, a conman engaged in identity theft, a hacker, or, in some instances, one family member in conflict with another.[40] Ironically, interoperable solutions as suggested in the GDPR[41] could aggravate security concerns at the expense of uniform rules and processes in this context. Although not seen as the main cause of the security vulnerabilities, interoperability is regarded as one of the factors that increase the number of opportunities for security breaches and the potential fall-out from such breaches.[42] Particularly for small and medium sized businesses (SME) with limited resources to invest in data security, this is a significant concern.

The Article 29 Working Party arguably has not succeeded in offering more clarity as to what security standards are expected. It places the responsibility for data security squarely on the current data controller, and suggests that risk mitigation measures may include "using additional authentication information, such as a shared secret, or another factor of authentication, such as a onetime password; suspending or freezing the transmission if there is suspicion that the account has been compromised; in cases of a direct

transmission from a data controller to another data controller, authentication by mandate, such as token-based authentications, should be used."[43]

It can be argued that more detailed guidance should be offered, in particular as regards the extent of responsibility and mandate a data controller has in assessing the security of the receiving controller and the ability of the data subject to keep the requested data secure. While 20 years of financial records can be reasonably expected to be safe when controlled by a bank, they are likely to be a lot less safe if downloaded as a spread sheet to an unprotected smartphone.

There are situations arguably where a data controller should have the right to refuse data portability due to concerns about security at the receiving end, hereunder uncertainty about the identity of the recipient and uncertainty surrounding the receiving data controller's ability to protect personal and third party data.

DATA PORTABILITY IN THE UNITED STATES

Data portability has been a contentious issue in the United States as well. The United States does not have a uniform data protection law similar to the European Union and there is no single regulatory authority dedicated to overseeing data protection law in the United States. Concerning the right to access data collected by companies the United States relies on a patchwork of state and sector specific federal laws for credit agencies and data brokers.[44] Furthermore, there are many guidelines, developed by governmental agencies and industry groups that are part of self-regulatory guidelines and frameworks that are considered "best practices, which are not legally binding.[45]

In the United States, the Federal Trade Commission is the federal privacy regulator regarding consumer protection, which also is relevant for the online environment.

Needles to say in the United States there is not a single provision that deals with the right to data portability, which is comparable to the European Union. In the United States, data portability generally is seen as an access to information/data issue.

The 1996 Health Insurance Portability and Accountability Act (HIIPA) is the first and most wide ranging data portability initiative giving individuals the right to access personal health information collected about them,[46] delivered, *e.g.*, on a storage device such as a USB drive. While offering the right to access data HIPAA does not currently address the need for controller–to–controller data portability.

In 2010, former US President Obama launched a series of initiatives entitled "My Data initiatives" to ensure that US citizens has easy and secure access to their own personal data.[47]

My Data Initiatives required the US Government to work together with the Federal Government, public and private sector to facilitate US citizens' access to their own personal data in a variety of sectors. As an example, Blue Button,[48] a data healthcare initiative, aimed to expand patients' access to their medical records so that data subjects can track their own health records and health information, which also can be shared with doctors and specialists.[49]

The Green Button[50] initiative allowed US citizens to access their detailed household or building electricity records in order to facilitate virtual energy audits with a view to identify inefficiencies and save money by switching providers.[51]

My Transcript[52] initiative allows data portability for the Internal Revenue Service and finally My Student[53] Data initiative allows US students to download information in relation to federal student grants and or loan information.

As pointed out by Macgillivray and Shambraugh, many private service providers have embraced data portability but there are still many other areas where data portability has not been required under US law and is not available in particular.[54]

On September 30, 2016, the Office of Science and Technology Policy (OSTP) asked various stakeholders their thoughts on the potential benefits and drawbacks of increased data portability, the industries that would most benefit and be harmed by increased data portability, the specific steps the Federal Government and private companies and others might adopt to encourage greater data portability and the best practices in implementing data portability.[55]

OSTP received 23 comments from several stakeholders including companies, trade associations, advocacy groups, and individuals.[56] Roughly half of the commentators limited their comments to health

data and data portability pertaining to it. Many commenters praised the potential benefits of data portability for users. The respondents suggested that an increased data portability would improve financial awareness, increase user exploration of new services, ease the burden of backing up data, increase user control and user trust and lower barriers to entry for services.[57] Some commentators raised concerns as to the cost of data portability and the increasing complexity of data portability between services due to the lack of commonly agreed standards.

Furthermore, some respondents suggested that data portability requirements might raise barriers to entry if they prove too be too burdensome to implement. One commentator summed up the views of several other commentators by stating that "portability should be incentivized but not mandated."[58] Some commentators suggested that mandatory data portability rules would be inefficient, ineffective and be premature for rapidly developing industries and this might have a negative impact on innovation.[59] Finally,respondents suggested that the government could incentivize data portability by increasing consumer awareness of it, leading by example or through encouraging interoperability and open standards, which would create the right environment for data portability.[60]

As data continues to increase in value both to users and service providers, ensuring data portability will become ever more crucial. From the above consultation, it is clear that data portability is quite desirable in the United States as well. Nevertheless based on the answers of the respondents it might be said that having a mandatory rule that applies across all sectors, is not very desirable for the industry stakeholders. Sarah Holland from Google illustrates this point and states that "one size fits all" requirements in relation to data portability may promote consistency but it is an ineffective approach, as it might create artificial barriers to new services entering the market place.[61] Arguably the right to data portability in the European Union and its successful implementation could prove useful in alleviating the concerns of the industry players.

The OSTP consultation and the responses obtained from various stakeholders provide very useful insights in relation to data portability in the US context. Nevertheless, it is worth noting that the OSTP consultation received only 23 responses and the majority of the responses were obtained from industry players and associations. This shows that there is a need for a more extensive consultation and debate in the United States, which takes into account the views of diverse stakeholders particularly consumers to have a more nuanced and more insightful review of the right to data portability.

CONCLUSION—WHAT LESSONS CAN BE DRAWN FROM THE EU EXPERIENCE

The objective of this article was to examine development of the right to data portability in the European Union under the GDPR with a view to establish whether any lessons can be drawn from the EU experience particularly for the United States.

As with the exception of sector specific regulation for the Health Sector (HIPAA) and voluntary programs, there is as of yet no such thing as data portability provision in the United States comparable to Article 20 of the GDPR. Hence a side-by-side comparison between the European Union and the United States is not relevant.

The GDPR is unprecedented in geographical reach and in scope, far surpassing any equivalent legislation anywhere in the world. The European Union currently is in uncharted territory as it sets out to break new ground in the area of data governance and in particular in the context of data portability rights for individuals. As such the European Union can offer the United States and other jurisdictions a wealth of insight as it explores ways of driving data portability across sectors.

First, the United States operates under the assumption that data portability is a choice for data controllers, not a right for data subjects. As such, much of the insight offered by the development of right to data portability under the GDPR has little relevance until the United States decides to see data portability as a fundamental right for data subjects. While the above-mentioned My Data Initiatives are commendable and certainly have driven innovation (although with limited adoption) in specific industries, they only apply to those industrial actors who see moral and economic sense in data portability and there is no penalty for not complying with these initiatives. In this regard, the first thing the United

States can take away from the data portability legislation in the GDPR may be as simple as: In the near future some form of legislation that comprises a right to data portability at federal level which applies to all industries and all firms, not just to a select few, is required. Such legislation does not need to be as rigid as the GDPR and can be shaped by taking into account the views of all relevant stakeholders including industry players and consumers.

Second, if and when the United States eventually decides to catch up and adopt data protection legislation, which includes a right to data portability they will benefit from second mover advantage, being able to walk in the steps of the European Union where advantageous, while avoiding known pitfalls. The GDPR is far from being perfect and arguably still a work in progress however the United States and other jurisdictions definitely will benefit from following the European discourse with regards to the definition of data observed by the data subject, the privacy rights of third parties, the possible need for enforcement pertaining to direct transfers between data controllers, the treatment of proprietary information and intellectual property rights, privacy and data security risks in transferring information in order to draw lessons.

Third, the United States probably will benefit from observing the agile process with which the GDPR, and maybe Article 20 in particular, has seen the light of day. The GDPR deals with new technological realities in fast moving markets. To expect perfection from the GDPR would be unrealistic. The combination of the GDPR combined with guidelines seems to be working very well in this context, offering a reasonably high degree of predictability in an emergent environment.

As the article demonstrates, the United States barely has started addressing data portability; nevertheless US firms will have to comply with the requirements of the GDPR in the European Union as of May 2018. While the main purpose of the GDPR is to give EU citizens control over their personal data, it has an extra territorial reach. The GDPR applies to any company that operates in the European Union. Hence a large amount of US businesses including Google, Facebook, Microsoft that collect data from EU data subjects need to comply with the GDPR to avoid hefty fines. In this respect, it is likely that the United States will soon have to engage with the need for convergence in global data protection and more specifically data portability policy.

For the European Union and the United States, important research themes are emerging. In the context of this article, three themes stand out.

First, in order to ensure successful enforcement of data portability there is a need to monitor and analyze the reasons offered by data controllers for refusal to comply with data portability requests, in particular relating to direct transfer between data controllers. This way, future guidelines can be adopted to address issues that hinder controller to controller data portability.

Second, interdisciplinary research is needed to ascertain the economic effects of data portability under the GDPR. As mentioned by several commentators,[62] personal data is the new oil. Hence legislating how an individual's personal data should be made available to other parties has wide ranging consequences and such legislation should be treated very cautiously. It is important to ascertain to what degree the data portability provision under Article 20 of the GDPR drives innovation, economic growth and consumer welfare, delivering on the promise of the European Digital Economy.

Finally, it is inspiring to see the results achieved by the US My Data initiatives such as Green Button. In this respect, the European Union would clearly benefit from research into what the United States gets right, in particular with reference to driving innovation and economic growth through constructive and transparent engagement with industry.

NOTES

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.
2. Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01 adopted on April 5, 2017.
3. This introduction borrows extensively from the author's earlier article on the right to data portability, *see* Aysem Diker Vanberg & Mehmet Bilal Unver, "The Right to data portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?" *European Journal of Law and Technology*, 8(1) (2017).
4. Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to processing of personal data and on the free movement of such data OJ L 281/31 (1995).
5. Sarah Downey, "The Most stringent data laws in the world: European Union agrees on penalties to protect personal data," *Legal Business*, December 16, 2015, *https://www.legalbusiness.co.uk/*

blogs/the-most-stringent-data-laws-in-the-world-european-union-agrees-on-penalties-to-protect-personal-data, accessed December 18, 2017.

6. Rhys Hadden, "The EU General data protection regulation: The new data protection landscape," *Guildhall Chambers*, May 2016, accessed December 18, 2017.
7. See for instance, Alexander Brown and Clare Adam, "The draft regulation–does every cloud have a silver lining?," 12(4) *P& DP* 9 (2012); Winston J. Maxwell, "Data Privacy: the European Commission pushes for total harmonisation," 18(6) *CTLR* 175 (2012).
8. *See* for instance, Nick Graham, "Data protection and privacy," 98 (Aug) *COB* 1 (2012); Sana Khan, "Practitioner's insight into the new EU Data Regulation," 5(1) *Comp& Risk* 6 (2016); Eduardo Ustaran, "EU General Data Protection Regulation: things you should know," 16(3) *P & DP* 3 (2016); Anita Bapat, "The new right to data portability," 13(3) *P & DP* 3 (2013); Francoise Gilbert, "European data protection 2.0: new compliance requirements in sight—what the proposed EU data regulation means for US companies," 28(4) *Santa Clara High Technology Law Journal* 815 (2001).
9. In this article the terms "individual," "consumer," "user," and "data subject" are used interchangeably to refer to a "data subject." According to Article 4 of the GDPR a "data subject" is an identifiable natural who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
10. Gabriela Zanfir, "The Right to Data Portability in the Context of Data Protection Reform," 2(3) *International Data Privacy Law* 149 (2012).
11. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.
12. Bapat, *supra* n.8.
13. The "Article 29 Working Party" is the short name of the Data Protection Working Party established by Article 29 of Directive 95/46/EC on data protection. It provides the European Commission with independent advice on data protection matters and helps in the development of harmonized policies for data protection in the EU Member States.
14. Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01 adopted on April 5, 2017 (hereinafter referred to as revised Guidelines on the right to data portability)
15. This section of the article borrows from the author's earlier article on the right to data portability, *see* Aysem Diker Vanberg & Mehmet Bilal Unver, "The Right to data portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?," *European Journal of Law and Technology*, 8(1) (2017).
16. Fablab Workshop is a workshop organized by the Article 29 Working Party in Brussels on July 26, 2016, with more than 90 participants including 40 representatives from Data protection Authorities. Among other issues the participants have discussed the issues relating to data portability. *See* Fablab, "GDPR/from concepts to operational toolbox, DIY," Results of the discussion (2016) available at *http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2016/20160930_fablab_results_of_discussions_en.pdf*, accessed December 18, 2017.
17. Fablab, *supra* n.16.
18. Inge Graef, Jeroen Verschaleken, Peggy Valcke, "Putting the right to data portability into a competition law perspective," *Law: The Journal of the Higher School of Economics, Annual Review* 4 (2013), available at SSRN: *http://ssrn.com/abstract=2416537*, accessed December 18, 2017.
19. *Id.*
20. Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, pages 9-10.
21. *Id.* at 10.
22. *Id.* at 11.
23. Barbara Engels, "Data portability amongst online platforms," 5(2) *Internet Policy Review* 4 (2016) at *http://policyreview.info/articles/analysis/data-portability-among-online-platforms*, accesed December 18, 2017.
24. Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, at 11.
25. *Id.* at 11- 12.
26. *Id.* at 18.
27. *Id.* at 16.
28. *Id.* at 16.
29. *Id.* at 15.
30. Peter Swire and Yianni Lagos, "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," 72 *Maryland Law Review* 335 (2013).
31. Laurits R Christensen, Andrea Colciago, Federico Etro, Greg Rafaert, "The Impact of the Data Protection Regulation in the EU," *European Financial Review* 72 (2013).
32. Swire and Lagos, *supra* n.30 at 379.
33. John Bowman, "New UK Minister's Data Protection To-Do List," (2015), *https://iapp.org/news/a/new-uk-ministers-data-protection-to-do-list/*, accessed December 18, 2017.
34. Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, at 15.
35. True Fit is footwear and apparel's discovery platform, which uses personal data obtained from users to enable them to find a better fit for clothing and footwear. The information on True Fit is available at *truefit.com*, accessed November 17, 2016.
36. Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, at 12.
37. *Id.*
38. Bapat, *supra* n.8 at 4.
39. *See* for instance Vanberg & Unver, *supra* n.3; *see also* Graef, Verschaleken, and Valcke, *supra* n.18.
40. Final report of the Federal Trade Commission Advisory Committee on Online Access and Security 19-25 (May 15, 2000), *https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf*, accessed December 18,, 2017; *see also* Swire and Lagos, *supra* n.30 at 374.
41. The GDPR, Recital 68.
42. Urs Gasser, "Interoperability in the digital ecosystem," Berkman Center Research Publication No. 2015-13 12 (2015), available at *SSRN http://ssrn.com/abstract=2639210* accessed December 18, 2017.
43. Guidelines on the right to data portability, Article 29 Working Party, [2017] 16/EN WP 242 rev. 01, at 19.
44. Samuel Grogan and Aleecia M. McDonald "Access Denied! Contrasting Data Access in the United States and Ireland," Proceedings on Privacy Enhancing Technologies (3) 192 (2016).
45. "Data Protection in the United States," Thomson Reuters Practical Law at *https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1* accessed December 18, 2017.
46. Grogan and McDonald, *supra* n.44.
47. Kristen Honey, Phaedra Chrousos, and Tom Black, "My Data: Empowering All Americans with Personal Data Access,"

https://obamawhitehouse.archives.gov/blog/2016/03/15/my-data-empowering-all-americans-personal-data-access, accessed December 18,, 2017.

48. More information on Blue Data initiative can be found online, *https://www.healthit.gov/patients-families/your-health-data*, accessed December 18,, 2017.
49. Honey, Chrousos, and Black, *supra* n.47.
50. More information on Green Button initiative can be found online, *https://energy.gov/data/green-button*, accessed December 18,, 2017.
51. Honey, Chrousos, and Black, *supra* n.47.
52. More information on My Transcript initiative can be found online, *https://www.irs.gov/individuals/get-transcript*, accessed December 18,, 2017.
53. More information on my student data information is available at *https://studentaid.ed.gov/sa/resources/mystudentdata-download*.
54. Alexander Macgillivray and Jay Shambaugh, "Exploring data portability, The White House Archives, *https://obamawhitehouse.archives.gov/blog/2016/09/30/exploring-data-portability*, accessed December 18, 2017.
55. *Id.*
56. *Id.*
57. White House Office of Science and Technology Policy Request for Information regarding data portability Public Responses (January 10, 2017), *https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/OSTP-Data%20Portability-RFI-Responses_for_humans.pdf*, accessed December 18,, 2017.
58. *Id.*; *see* respondent Jordan Gross, U.S. Chamber Technology Engagement Center, pp. 29.
59. White House Office of Science and Technology Policy Request for Information regarding data portability Public Responses, *supra* n.57. On this point *see* the respondent Sarah Holland, Google at page 32.
60. *Id.*
61. *Id.*
62. *See* for instance, Meglena Kuneva, "Roundtable on Online Data Collection, Targeting and Profiling," SPEECH/09/156, *http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm*, accessed December 18, 2017.